

U.S. Appl. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

Listing of Claims

1. (Currently Amended) A data processing apparatus comprising:
encrypting means for encrypting compressed data blocks into respective in-units
of an encryption block having a predetermined data length;
processing means for defining a plurality of processing blocks, each processing
block having a data block length of a whole multiple of said predetermined length of said
encryption block and for expanding compressed data blocks in units of said predetermined into
one processing block length,

wherein said encryption block is configured to not straddle any of said plurality of
processing blocks;

storage means for storing the encrypted data; and
control means for writing the encrypted data in said storage means so that the data
said compressed data blocks positioned in the same encryption block is arc also positioned in the
same processing block, said control means reading the data from said storage means in units of
the processing block,

wherein said stored encrypted data is compressed into minimum readable data
units such that there are no breaks between the stored encryption blocks and the processing load
to access the data is thereby reduced when accessing encrypted audio data stored in said storage
means.

BEST AVAILABLE COPY

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

2. (Original) The data processing apparatus as set forth in claim 1, wherein said control means inserts data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

3. (Original) The data processing apparatus as set forth in claim 1, wherein said encrypting means performs encryption processing using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted.

4. (Original) The data processing apparatus as set forth in claim 3, wherein said control means manages the encrypted data stored in said storage means using a cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

5. (Original) The data processing apparatus as set forth in claim 4, wherein said control means stores said one or more processing blocks at consecutive addresses of said storage means in the order of encryption, stores said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption, and stores said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

6. (Original) The data processing apparatus as set forth in claim 1, wherein said control means outputs said data read out in processing block units to said processing means.

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

7. (Canceled)

8. (Currently Amended) A data processing system for inputting and outputting data while performing mutual identification between a storage apparatus and a data processing apparatus, said storage apparatus comprising:

first mutual identification processing means for performing processing for mutual identification with said data processing apparatus;

storage means for storing said data; and

first control means for allowing the input and output of data between said data processing apparatus and said storage means when said data processing apparatus is recognized to be a legitimate party by the processing for mutual identification;

said data processing apparatus comprising:

second mutual identification processing means for performing processing for mutual identification with said storage apparatus;

encrypting means for encrypting compressed data blocks into respective in-units of an encryption block of a predetermined data length;

processing means for defining a plurality of processing blocks, each processing block having a data block length that is a whole multiple of the predetermined data length of the encryption block and for expanding compressed data blocks into in-units of said predetermined one processing block length,

wherein said encryption block is configured to not straddle any of said plurality of processing blocks; and

second control means for performing at least one of write processing and read

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

processing when said data processing apparatus is recognized to be a legitimate party by the processing for mutual identification, for writing the encrypted data in said storage means so that said compressed data blocks positioned in one encryption block ~~is-are~~ also positioned in the same processing block during write processing,

and for reading the data from said storage means in units of a processing block during read processing,

~~wherein said stored encrypted data is compressed into minimum readable data units such that there are no breaks between the stored encryption blocks and the processing load to access the data is thereby reduced when accessing encrypted audio data stored in said storage means.~~

9. (Original) The data processing system as set forth in claim 8, wherein said second control means inserts data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

10. (Original) The data processing system as set forth in claim 8, wherein said encrypting means performs encryption processing using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted.

11. (Original) The data processing system as set forth in claim 10, wherein said second control means manages the encrypted data stored in said storage means using a

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

12. (Original) The data processing system as set forth in claim 11, wherein the second control means stores said one or more processing blocks at consecutive addresses of said storage means in the order of encryption, stores said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption, and stores said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

13. (Currently Amended) A data processing method, comprising the steps of:
 encrypting compressed data blocks into respective in-units of an encryption block having a predetermined data length;
 defining a plurality of processing blocks, each processing block having a data block length that is a whole multiple of the predetermined data length of the encryption block,
 wherein said encryption block is configured to not straddle any of said plurality of processing blocks;
 expanding compressed data blocks in units of said predetermined into one processing block-length;
 writing the encrypted data to a storage means so that compressed data blocks all of the data positioned in one encryption block is are also positioned in the same processing block; and
 reading the data from the storage means in units of the processing block.

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

~~wherein said stored encrypted data is compressed into minimum readable data units such that there are no breaks between the stored encryption blocks and the processing load to access the data is thereby reduced when accessing encrypted audio data stored in said storage means.~~

14. (Original) The data processing method as set forth in claim 13, further comprising the step of inserting data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

15. (Original) The data processing method as set forth in claim 13, further comprising the step of using the encryption block to be encrypted and a cipher text obtained from the encryption of the encryption block immediately prior to the encryption block to be encrypted to perform encryption processing.

16. (Original) The data processing method as set forth in claim 15, further comprising the step of managing the encrypted data stored in said storage means using a cluster containing one or more processing blocks and values initially used when encrypting an encryption block in one of said processing blocks.

17. (Original) The data processing method as set forth in claim 16, further comprising the steps of :
storing said one or more processing blocks at consecutive addresses of said

U.S. Appln. No. 09/524,358
Reply to Office Action dated February 24, 2006

PATENT
450100-02402

storage means in the order of encryption;

storing said one or more encryption blocks in said processing blocks at consecutive addresses of said storage means in the order of encryption; and

storing said initial values at an address immediately prior to the address of at which the first encryption block in the cluster is stored.

18. (Original) The data processing method as set forth in claim 13, further comprising the step inserting data into said processing block to adjust the data length in the processing block so that the length of said processing block becomes a whole multiple of the predetermined data length of said encryption block.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.